

# CLARK HILL

---

Robert A. Stern  
T 312.985.5940  
F 312.985.5955  
Email: rastern@clarkhill.com

Clark Hill  
130 East Randolph Street  
Suite 3900  
Chicago, IL 60601  
T 312.985.5900  
F 312.985.5999

[clarkhill.com](http://clarkhill.com)

September 12<sup>th</sup>, 2019

**Attorney General Gordon MacDonald**  
**Office of the Attorney General**  
**33 Capitol Street**  
**Concord, NH 03302**  
[attorneygeneral@doj.nh.gov](mailto:attorneygeneral@doj.nh.gov)

Dear Attorney General MacDonald:

We represent Envista Forensics, LLC (“Envista”) with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. Envista is committed to answering any questions you may have about the data security incident, its response, and has taken steps to prevent a similar incident in the future.

## **1. Nature of security incident.**

On January 24<sup>th</sup>, 2019, Envista became aware that an unauthorized individual may have accessed one corporate email account. Immediately after discovering the suspicious activity, the account owner’s password was changed, the computer was removed from service, and Envista began to investigate the suspicious activity. Envista forensically confirmed that there was unauthorized activity into one email account and subsequently hired an external resource to conduct a manual review of the account for personal information. The manual review of the account was completed and Envista was provided a written output file for to use for notification purposes. The personal information contained in the impacted email inbox was limited to employee personal information. While we have no evidence that this information was accessed or acquired by the unauthorized individual, Envista issued notice to the potentially impacted employees out of an abundance of caution. The personal information contained in the email account involved some combination of an employee’s name, address, Social Security number, passport information, and financial account information Letters notifying the potentially affected individuals were subsequently mailed on July 19<sup>th</sup>, 2019.

The letter included details about the security incident, the three major credit reporting agencies, and offered complimentary credit monitoring services through IDExperts. Envista also provided employees with contact information for any questions.

September 12<sup>th</sup>, 2019

Page 2

**2. Number of New Hampshire residents affected.**

One New Hampshire resident may have been affected and was notified of the incident. A notification letter was sent to the potentially affected individual on July 19<sup>th</sup>, 2019 via regular mail (a copy of the form notification letter is enclosed).

**3. Steps taken or plan to take relating to the incident.**

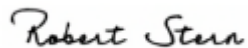
Steps have been taken to help prevent a similar occurrence in the future. Envista has now implemented multi-factor authentication on all of its systems, conducted a penetration test on its environment, and updated its password policy to require more complex passwords. Additionally, Envista has terminated the employee whose account was accessed for failing to follow proper security protocol and has offered one year of credit monitoring and identity restoration services through ID Experts.

**4. Contact information.**

Envista takes the security of the information in its control seriously, and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at [Rastern@clarkhill.com](mailto:Rastern@clarkhill.com) or (312) 985-5940.

Very truly yours,

CLARK HILL



Robert A. Stern

Enclosure



111 Deer Lake Road, Suite 100  
[REDACTED]  
Deerfield, IL 60015

To Enroll, Please Call:  
**1-800-939-4170**  
Or Visit:  
<https://app.myidcare.com/account-creation/protect>  
Enrollment Code: [REDACTED]

June 28, 2019

[REDACTED]

### Envista Forensics Data Security Incident

[REDACTED]:

We are writing to notify you of a data security incident experienced by Envista Forensics, LLC that may have impacted your personal information, including your name and Social Security number. We value and respect the privacy of your information and we sincerely apologize for any concern or inconvenience this may cause you. This letter contains steps you can take to protect your information and the resources we are making available to help you.

#### 1. What happened?

We recently detected suspicious activity associated with an employee email account. We changed the password for the email account and had computer forensic experts to help us investigate how the incident occurred and whether any information in the account was at risk. The forensic investigation revealed that an unauthorized person had access to an employee's email account for a short period of time. Our forensic investigator informed us that your information may have been stored in the account. While we believe misuse of your information is unlikely, we wanted to let you know about this incident out of an abundance of caution. While we believe misuse of your information is unlikely, we wanted to let you know about this incident out of an abundance of caution. From our review, this information may include your name, and Social Security number. For a very limited number of people, your date of birth and passport number may have been affected as well.

#### 2. What we are doing and what you can do:

Because we value the privacy and security of your information, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

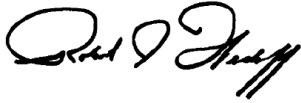
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling **1-800-939-4170** or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 5 am - 5 pm Pacific Time. Please note the deadline to enroll is June 10, 2020.

We want to assure you that we are taking steps to prevent this type of incident from happening in the future. We have retrained our employees on recognizing and appropriately responding to suspicious emails and other security threats. We are also reviewing and revising our security policies and have updated our password policy to require more complex passwords for each employee. We encourage you to review the additional information contained in this letter about protecting your identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

**3. For more information:**

If you have any questions or concerns, please reach out to Justin Hunter at [Justin.Hunter@EnvistaForensics.com](mailto:Justin.Hunter@EnvistaForensics.com). Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Robert Wedoff". The signature is fluid and cursive, with the first name "Robert" and last name "Wedoff" clearly distinguishable.

**Robert Wedoff**  
**President**  
**Envista Forensics, LLC**

## Recommended Steps to help Protect your Information

- 1. Website and Enrollment.** Go to <https://app.myidcare.com/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.alerts.equifax.com](http://www.alerts.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection (<http://www.ca.gov/Privacy>) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.